Report No. D-2010-085 September 22, 2010

Inspector General
United States Department of Defense

Kuwait Contractors Working in Sensitive Positions Without Security Clearances or CACs

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
22 SEP 2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Kuwait Contractors Working in Sensitive Positions Without Security Clearances or CACs	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Defense Inspector General,400 Army Navy Drive,Arlington,VA,22202**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**38**	

Additional Information and Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (703) 604-8932, or by mail:

ODIG-AUD (ATTN: Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms and Abbreviations

AR	Army Regulation
CAC	Common Access Card
CAR	Corrective Action Request
CSA	Combat Support Associates
CSSC-K	Combat Support Services Contract-Kuwait
DCMA	Defense Contract Management Agency
OIG	Office of Inspector General
PCO	Procuring Contracting Officer
QAR	Quality Assurance Representative
RICC	Rock Island Contracting Center
SCAR	Security Clearance Access Roster
SOW	Statement of Work

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

September 22, 2010

MEMORANDUM FOR DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Kuwait Contractors Working in Sensitive Positions Without Security Clearances or CACs (Report No. D-2010-085)

We are providing this report for review and comment. We considered management comments on a draft of this report when preparing the final report. This audit focused on management of the Combat Support Services Contract-Kuwait, the contractor's security program, and contractor employee security clearances. We identified contractors in Kuwait working in sensitive positions without the required security clearances or common access cards. Improvements are necessary to mitigate the security risks to the military, civilian, and contractors in Kuwait.

DOD Directive 7650.3 requires that recommendations be resolved promptly. The Commander, Defense Contract Management Agency-Kuwait, comments were partially responsive to Recommendation 2.c. Therefore, we request additional comments on Recommendation 2.c by October 22, 2010.

If possible, send a .pdf file containing your comments to audacm@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-9071 (DSN 664-9071).

Bruce Burton
Deputy Assistant Inspector General
Acquisition and Contract Management

Results in Brief: Kuwait Contractors Working in Sensitive Positions Without Security Clearances or CACs

What We Did

This is the first in a series of reports on the Combat Support Services Contract-Kuwait (CSSC-K). We reviewed the CSSC-K contract to identify potential weaknesses related to the management of the contractor's security program and contractor employee security clearances. Contractor employees in sensitive positions without security clearances is not acceptable and poses a security risk for military, civilian, and contractors in Kuwait. The CSSC-K contract was awarded in 1999 and had a value of more than $3.3 billion. Unless extended for a third time, the contract will end September 30, 2010, but the corrective actions identified in this report must be established and implemented in follow-on contracts.

What We Found

CSSC-K contractor employees worked in sensitive positions without the required security clearance. Combat Support Associates (CSA), the CSSC-K contractor, had employees in sensitive positions with no record of security clearances or without valid clearances, an incorrectly identified sensitive position, and incomplete security files. CSA officials also allowed contractor employees to remain in sensitive positions without a security clearance after they were informed they were in violation of the contract. Lastly, the Army did not ensure all contractors had the common access cards (CACs) required for base access. This occurred because CSA officials did not identify and track all positions or obtain the required clearance for all employees. Additionally, the Defense Contract Management Agency (DCMA) did not provide oversight of the contractor's security program in accordance with the contract or DCMA's Theater Quality Plan.

What We Recommend

Among other recommendations, we made the following to the Commander, DCMA-Kuwait, and the Procurement Contracting Officer:

- require quality assurance representatives to review security files and issue corrective action reports,
- remove contractors working in sensitive positions without security clearances or CACs,
- implement contractual remedies to recoup any money paid for services not provided,
- require the contractor to conduct quarterly reviews to validate the Security Clearance Access Roster,
- consider debarment of the contractor,
- verify that the human resources listings include all employees in sensitive positions, and
- coordinate with the Kuwait bases Provost Marshall Offices to conduct a review to verify all contractor employees have a CAC.

Management Comments and Our Response

The Acting Executive Director, Rock Island Contracting Center, and Commander, DCMA-Kuwait, either agreed with the recommendations or were partially responsive. Therefore, we require additional comments. Please see the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Commander, Defense Contract Management Agency-Kuwait	2.c	2.a and 2.b
Procuring Contracting Officer, Rock Island Contracting Center		1.a, 1.b, 1.c, 1.d, 1.e, 1.f, and 1.g

Please provide comments by October 22, 2010.

Table of Contents

Introduction

Objectives

This is the first in a series of audit reports on the Combat Support Services Contract-Kuwait (CSSC-K) contract. We determined whether DOD properly managed and administered the contract supporting base operations in Kuwait. Specifically, we determined whether the contract management and administration personnel complied with Federal and DOD policies. This report focuses on the management of the contractor's security program and contractor security clearances. For a discussion on the Scope and Methodology, please see the Appendix.

We performed this audit pursuant to Public Law 110-181, "National Defense Authorization Act for FY 2008," section 842, "Investigation of Waste, Fraud, and Abuse in Wartime Contracts and Contracting Processes in Iraq and Afghanistan," January 28, 2008. Section 842 requires

> …thorough audits to identify potential waste, fraud, and abuse in the performance of (1) Department of Defense contracts, subcontracts, and task and delivery orders for the logistical support of coalition forces in Iraq and Afghanistan; and (2) Federal agency contracts, subcontracts, and task and delivery orders for the performance of security and reconstruction functions in Iraq and Afghanistan.

Background

The CSSC-K contract (DASA02-99-C-1234) supports all base operations in Kuwait. The CSSC-K contract is a cost-plus-award-fee contract that was awarded in 1999 to Combat Support Associates (CSA). The contract term was for a base year and 9 option years. The original contract award ceiling, including all option years, was for $503,808,483, but due to the increase in military efforts in Southwest Asia, the value increased to more than $3.3 billion as of May 2010, with 355 contract modifications. CSA is a joint venture between AECOM, Aleut Corporation, and Research Analysis and Maintenance, Incorporated.

The CSSC-K contract is ending, but the corrective actions identified in this report must be established and implemented in follow-on contracts. The last option year for the CSSC-K contract ended September 30, 2009; however, Rock Island Contracting Center (RICC) officials extended the contract two additional times. Unless RICC officials extend the contract for a third time, the CSSC-K contract will end September 30, 2010. RICC officials stated that the CSSC-K contract will be separated into three follow-on contracts: Kuwait Base Operation Security Support Services, Ammunition Supply Point, and Supply Support Activity.

The Army Contracting Command-Kuwait managed the CSSC-K contract from its inception until November 2007 when, due to fraud and quality issues in contracting overseas, the Secretary of the Army transferred the management of the CSSC-K contract

to RICC. Little can be determined about the contract management from 1999 to 2007 as documents were not well maintained before the contract transferred to RICC. RICC officials encountered many issues when it took over management of the contract, including undefinitized contract actions, a statement of work (SOW) that did not include all contract requirements, and inadequate property inventories.

RICC officials delegated contract administration responsibilities to the Defense Contract Management Agency (DCMA). DCMA has a presence in Kuwait and oversees the day-to-day operations of the contract. DCMA officials coordinate with the procuring contracting officer (PCO)[1] at RICC to keep the PCO informed of the CSSC-K contract operations.

Review of Internal Controls

DOD Instruction 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, requires DOD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses within the Rock Island Contracting Center and the Defense Contract Management Agency for the management and oversight of the security program supporting the CSSC-K contract. Implementing recommendations in the Finding will improve CSA's security program. We will provide a copy of the report to the Rock Island Contracting Center and DCMA senior officials responsible for internal controls.

[1] While the FAR uses the term "contracting officer," RICC uses the terms "procuring contracting officer" and "administrative contracting officer" to cover the contracting officer functions. Therefore, in this series of reports, we use the terms procuring contracting officer and administrative contracting officer and not contracting officer.

Finding. Contractor Fails to Fully Implement Security Clearance Requirements

CSSC-K contractor employees occupied sensitive positions such as force protection officers, system administrators, and supply inspectors in Kuwait without obtaining security clearances as required in the CSSC-K contract, DASA02-99-C-1234. Specifically, CSA had:

- 21 of 379 employees in sensitive positions who were not tracked by CSA's security office;
- 11 of 379 employees in sensitive positions who did not have a valid security clearance;
- at least 1 employee in a sensitive position that CSA officials classified as nonsensitive; and
- incomplete information in 41 of 49 security files reviewed.

Additionally, CSA officials allowed 20 employees to remain in sensitive positions without the required security clearance after its internal quality assurance office and DCMA officials informed CSA officials that they were in violation of the contract. Further, the Army and PCO did not ensure that 36 contractor employees who had no record of a security clearance, no valid security clearance, or no security file, had the common access cards (CACs)[2] required for base access and that those CACs had the proper restrictions to prohibit contractor access to restricted areas or systems. This occurred because CSA officials did not identify and track all sensitive positions or obtain the required security clearances. Additionally, DCMA officials did not provide oversight of the contractor's security program in accordance with the contract or the Theater Quality Plan. If DCMA and contractor officials do not ensure that all employees have the required security clearances and maintain proper security information, they jeopardize the military mission and threaten the safety and security of the military, civilian, and contractor personnel in Kuwait. This issue is particularly timely and relevant in identifying security concerns that the PCO must ensure are correctly implemented in the new Kuwait-Base Operation Security Support Services, Ammunition Supply Point, and Supply Support Activity contracts.

DOD Personnel Security Program

DOD Directive 5200.2, "DOD Personnel Security Program," April 9, 1999, requires that access to classified information or assignment to sensitive duties must be granted only to United States citizens with a completed investigation. The background investigation is required to show that contractor employees are reliable and trustworthy and that there is no reason to doubt their ability to protect classified information or their allegiance to the United States. According to DOD 5200.2-R, "Personnel Security Program," updated

[2] A CAC is an identification card that used to gain access to DOD resources, installations, and sensitive information.

February 23, 1996, sensitive positions are those civilian positions within DOD that include duties of a sensitive nature and access to classified information where the misconduct of personnel in that position could result in an unacceptable impact on national security.

DOD 5200.2-R and Army Regulation (AR) 380-67, "Personnel Security Program," September 9, 1988, further state that contractor personnel who are employed by DOD may be considered for access to classified information only when such access is required in connection with official duties. AR 380-67 states that only heads of DOD Components for critical-sensitive positions and organizational commanders for noncritical-sensitive positions can designate a position as sensitive.

Contractor Positions Lack Security Clearances

CSSC-K contractors occupied sensitive positions; however, the PCO did not ensure that all sensitive positions were designated by the proper officials as outlined in AR 380-67 or that CSA officials provided justification for which positions they claimed required a security clearance. The contractor is responsible for staffing sensitive positions with employees who have security clearances, tracking security clearances, and maintaining records. The SOW, as a part of the contract, required the contractor to maintain security clearances for employees involved in inspections, repairs, or maintenance for classified equipment or parts; who handle classified information in any format; or who have access to restricted areas. The SOW further required CSA officials to provide the Army with a list of contractor employees who required security clearances. The SOW required the contractor to update the list and provide it to the Army as changes occurred. However, while the contract required CSA officials to create and maintain a list of contractor employees who require a security clearance, RICC and DCMA officials failed to provide oversight and validate whether the decisions made by the contractor for these positions were in accordance with the SOW.

Based on discussions with CSA officials, they did not think the Army clearly defined all requirements in the SOW. According to CSA's human resources information system analyst, the Army did not clearly define or designate all sensitive positions; therefore, CSA officials relied on their own department managers to determine which positions required a security clearance. CSA's facility security branch manager stated her office tracked all employees that officials designated as requiring a clearance through CSA's security clearance access roster (SCAR). CSA's quality assurance manager stated that CSA's human resources office maintained a list of all positions that required a security clearance and the individuals in each position. According to a CSA official, the human resources list populated the SCAR through an electronic transfer from CSA's human resources system. However, the facility security branch manager stated that no one verified that all sensitive positions were captured on the human resources list or even that the human resources list matched the SCAR since it was automatically populated. Additionally, since RICC and DCMA officials did not validate CSA's list of sensitive positions, they do not know whether the SCAR or human resources list was all inclusive. Further, CSA officials did not request that the PCO clarify which positions required a

security clearance even though they believed the PCO did not define all sensitive positions. As a result, CSA officials did not comply with the contract requirements.

SOW Security Clearance Requirements Disregarded

CSA's security program officials did not obtain security clearances, as required in the SOW, for all employees in sensitive positions. We reviewed CSA's list of 379 employees working in sensitive positions and identified 21 contractor employees who were not tracked by CSA's security office and 11 contractor employees who did not have a valid security clearance. Contractor employees working in a position that require a security clearance typically earn a higher salary than those in positions that do not require clearances. Therefore, CSA officials may have billed the Army based on rates that were commensurate with employees occupying sensitive positions who should have possessed a clearance when, in fact, these employees did not possess a clearance.

Failure to Track Security Clearances

We identified 21 contractor employees in sensitive positions who were not tracked by the contractor's security office. We compared the SCAR to the human resources list of 379 employees working in sensitive positions who required a security clearance to ensure all employees were on the SCAR. Twenty-one of the 379 employees on the human resources list were not on the SCAR. The facility security branch manager told us that 20 of the 21 employees identified did not yet occupy the positions and that is why those individuals were not on the SCAR. However, the CSA human resources systems manager stated that the facility security branch manager was incorrect and that if the name was on the human resources list then the individual was already working in that position. Therefore, CSA employees were working in positions that required a clearance but CSA officials did not track whether the employees had a security clearance. Some of the positions the 21 employees occupied included Theater Redistribution Center inspectors and supply technicians, both of which handled sensitive materials, as well as a force protection officer responsible for security of the military base. Therefore, the 21 contractor employees had access to sensitive materials. The PCO should require CSA officials to validate whether these contractor employees have the required clearance. Those that are lacking the clearance should be removed from their positions.

Questionable Security Clearance Status

We identified 11 employees who did not have a clearance because their clearances were either in a "hold" or "interim declined" status. Six of the 11 employees were in sensitive positions even though their clearances were on hold. According to CSA's facility security branch manager, the hold designation meant that the individual's security clearance had not yet been approved. These employees occupied sensitive positions such as a Theater Redistribution Center inspector, a help desk technician, and force protection officers. The remaining five employees occupied sensitive positions with an interim declined clearance. According to CSA's facility security branch manager, the interim declined status indicated that the employee's clearance was declined during his or her interim clearance review but had not yet received a determination on the full security clearance. Employees working in an interim declined status included a Theater Redistribution Center inspector, a supply technician, a systems administrator, a supply

supervisor, and a security supervisor. The systems administrator accessed systems with sensitive information and may have had responsibilities such as installation/configuration, operations and maintenance of systems hardware, software, and related infra-structure. These 11 contractor employees were working in sensitive positions without a valid security clearance, clearly a security violation. The PCO should direct CSA officials to immediately remove these 11 contractor employees from their positions until they obtain the required security clearance.

Positions Required Clearances Not Tracked

As already noted in this report, sensitive positions should be identified in the contract, CSA's human resources list, and the SCAR, and employees in these positions must have security clearances. However, no one verified whether CSA officials tracked all positions that require a clearance. Further, CSA's security manager informed us that when CSA employees identified an employee working in a sensitive position without a clearance, CSA officials created a "mirror" position for that person until they obtained their clearance. The CSA security manager stated a mirror position was the exact same position, only CSA officials did not allow that person access to sensitive information. However, CSA's security manager stated that CSA officials relied on the individual's department manager to ensure that person did not have access to sensitive information but no one verified whether this was being done. Additionally, since the person was designated as occupying a position without a security clearance, he or she would not appear on the SCAR for additional monitoring. While DCMA officials verified whether contractor employees had necessary clearances by reviewing the SCAR, it had no basis to determine if the SCAR included all required positions.

We identified an individual working in a sensitive position that was not identified on the human resources list of sensitive positions, but the SOW required the person occupying the position to have a clearance. This individual was a supervisor in the Joint Military Mail Terminal with oversight of employees who scan all packages sent to the military base, and must report and dispose of any items identified that are not allowed. The employee also had access to sensitive packages that were locked in a secure room. The SOW required any person handling registered mail to have a security clearance. We asked CSA's human resources information systems analyst why this position was not on the list and he replied that the position could have been labeled incorrectly, but he acknowledged that it should have been on the list.

DCMA officials and CSA officials informed us that they had identified issues with employees stealing items, such as alcohol, drugs, and weapons from packages while working in the Joint Military Mail Terminal. Therefore, DCMA officials should have reviewed the human resources list of sensitive positions for the Joint Military Mail Terminal supervisor position. The supervisor did have a security clearance; however, this individual was not on the SCAR because his position number was incorrectly labeled by human resources employees. Therefore, CSA's security office was not tracking security information for this individual. While we found only one instance where the position was labeled incorrectly, there could be others since the PCO and DCMA officials did not validate whether CSA officials tracked all positions that required a clearance. The PCO

should conduct a 100 percent review of all positions and designate each position either sensitive or nonsensitive and the security clearance level, if required. The PCO should further require DCMA officials to periodically validate whether CSA's list of contractor employees in sensitive positions is all inclusive.

Contractor Security Files Missing Documents

The CSSC-K contract SOW required that CSA officials implement and maintain a security program. The SOW stated that the security program must include obtaining security clearances for contractors. The contract further required CSA officials to develop standard operating procedures for its security program.

To obtain a security clearance, DOD 5200.2-R requires the individual to validate that he or she is a U.S. citizen. Additionally, DOD 5200.2-R requires that all persons cleared for access to classified information or assigned to duties requiring a clearance must be given an initial security briefing and sign an SF 312, "Classified Information Nondisclosure Agreement" (SF 312). Further, CSA's standard operating procedures required that every personnel file include the SOW section that justifies that the position requires a security clearance, the employee's position description, a copy of a passport, signed nondisclosure agreements, overseas operational security briefing memoranda, and a joint personnel adjudication system printout to show the individual's clearance level. However, CSA's security files did not include all required information, and CSA officials did not maintain files for all contractor employees required to have a security clearance.

We reviewed 49 of 379 contractor employee security files for the required documents listed above and found that only 8 of the 49 files had all of the documents required by DOD 5200.2-R and by the contractor's standard operating procedures. The other 41 of 49 files did not include 1 or more of the required documents. Specifically, of the 49 employee files reviewed:

- 8 did not include a copy of a passport,
- 16 did not include a signed copy of the SF 312,
- 13 did not include a signed copy of the overseas operations security briefing memorandum,
- 30 did not include the applicable SOW section,
- 20 did not include the position description justifying the need for the security clearance, and
- 6 did not include proof of their clearance level (these were the same 6 employees with a clearance in a hold status).

Four of the eight employees with no evidence of a passport worked in the security services department. Without a passport, there was no evidence that the employees were U.S. citizens as required by DOD 5200.2-R. Additionally, unless CSA officials obtain a signed SF 312 and proof of the security briefing for the employees without this information, the PCO should take actions to have their clearances revoked per DOD 5200.2-R and direct CSA officials to remove them from their positions. Further, because there were files without an applicable SOW section and position description, we

could not validate that CSA officials justified whether access to sensitive information was required in connection with official duties, as stated in DOD 5200.2-R.

CSA's security branch manager could not provide 4 of the 49 requested employee files and could not verify whether those four contractors had the required clearance for their position. The four employees were the chief operating officer, a range safety technician, and two force protection officers, all of whom had access to sensitive information. While CSA officials failed to meet the SOW requirements, the PCO and DCMA officials were responsible for taking appropriate action against CSA officials. The PCO should direct CSA officials to reconstitute the employee personnel files and validate that each employee had a security clearance. If CSA officials find they do not have a security clearance, they should terminate the employee immediately. Further, those terminated employees must be required to turn over their CAC, and the PCO should recoup the employee salaries since they were not fulfilling SOW requirements.

DCMA Oversight Failed

DCMA-Kuwait officials are responsible for monitoring the contract to ensure that services performed by the contractor are in compliance with the contract. DCMA-Kuwait officials failed to provide oversight of the contractor security program to ensure it complied with contract requirements outlined in the SOW. Specifically, DCMA officials did not review CSA's maintenance of the security files to verify that contractor employees CSA officials claimed had a security clearance actually had the clearance. The DCMA quality assurance representative (QAR) responsible for oversight of security informed us that DCMA officials ensured that the contractor positions that require a clearance were occupied by contractor employees with clearances. The security QAR stated that he reviewed the SCAR, verified a sample of position descriptions, and reviewed information in the Joint Personnel Adjudication System for a sample of employees to validate that the information in SCAR was correct. However, the QAR could not provide documentation to support his statements that the reviews were conducted. The SCAR did not include all contractor employees in sensitive positions and all contractor employees did not have the required security clearances. We asked the QAR why he did not review the supporting employee files to verify contractor security clearances, and he stated that the contract did not direct the contractor to maintain the security files. Therefore, according to the QAR, since it is not required in the contract, it is not one of DCMA's delegated responsibilities. However, the contract's SOW requires that the contractor obtain and maintain security clearances. DOD 5200.2-R requires the supporting documentation for employees who have a security clearance; therefore, the supporting documents in the security files are required for obtaining a security clearance and should be reviewed by DCMA officials. DCMA officials should review CSA's list of contractor positions to verify that the list is all-inclusive and compare that list to the SCAR to validate that CSA officials track all employees who require a security clearance. CSA employees are required by the contract to obtain a security clearance; therefore, the PCO should ensure that DCMA officials review the supporting files to verify that all contractors in sensitive positions have the required clearances. CSA placed their employees in sensitive positions, such as Theater Redistribution Center inspector, supply technician or supply supervisor without the required security clearances, clearly a

security violation. Until DCMA officials review all CSA employees and verify whether they have the security clearance required for each position, the PCO should suspend employees that do not have the required security clearances commensurate with their position. If DCMA officials choose to verify contractor clearance information in the Joint Personnel Adjudication System instead of looking at the files, DCMA officials must document these reviews.

Contractor's Noncompliance With the SOW

CSA officials continued to staff 20 employees without clearances in sensitive positions after being notified by its quality assurance office and DCMA officials of their non-compliance with the SOW requirements. According to FAR Subpart 9.406, "Limitations," when contractors are in willful violation of their contract, the PCO can pursue debarment of the contractor. There was confusion on this matter because DCMA officials did not issue a corrective action request (CAR) as required. DCMA officials did not issue a CAR because they relied on CSA's quality assurance officials to issue their own internal CAR on the issue. However, CSA officials caused further confusion when they developed a corrective action plan for their internal CAR that was tied to an unrelated DCMA CAR. Subsequently, DCMA officials closed the CAR and stated CSA officials implemented all corrections; however, CSA officials did not. Therefore, not only did CSA officials violate the contract because they did not comply with the SOW, but DCMA officials did not conduct oversight of this issue in accordance with its Theater Quality Plan.

Oversight Lacking on Security Programs

In May 2009, CSA officials issued an internal CAR stating that CSA officials failed to comply with facility and physical security requirements stated in the SOW. CSA's quality assurance office attributed the noncompliance to a lack of oversight of the facility and physical security program by CSA management. CSA's quality assurance office developed a corrective action plan to address the issue that included: reviewing the SOW for positions that require security clearances to ensure the positions were properly reflected in the human resources information system database, validating that those employees had a security clearance, and verifying that no potential or current employee was hired or reassigned to a position that required a security clearance unless he or she had an approved security clearance or authorization. CSA officials closed its internal CAR on October 5, 2009, after DCMA officials reported that CSA officials had implemented all of the corrective actions. However, we found that the issues were not corrected.

While CSA officials admitted CSA did not comply with the SOW, the CSA quality assurance manager stated that the 20 employees were awaiting a final determination from the PCO on whether the positions required clearances. Despite notice from DCMA-Kuwait officials and the CSA internal CAR, CSA officials continued to staff sensitive positions with employees without security clearances. CSA officials violated the contract requirements and the PCO should pursue debarment of the contractor in accordance with FAR Subpart 9.406. While this report addresses areas where CSA

officials did not comply with the contract on security issues, the next report in this series will address CSA compliance with other contract requirements.

DCMA Missed Opportunity to Enforce Contract

DCMA officials are required to issue a CAR in accordance with their Theater Quality Plan when they identify that contractor performance is not in compliance with the contract. The DCMA CAR must outline the issues identified by the QAR and require the contractor to develop a corrective action plan. The corrective action plan must outline how the contractor will fix the issue and the projected milestones.

One of the DCMA QARs stated that DCMA officials identified issues with CSA officials not knowing which positions required a security clearance. The QAR provided DCMA audit reports showing that, in May 2009, DCMA officials identified 55 contractor employees working in sensitive positions without a security clearance which, according to the reports, had been an issue since February 2008. The CSA quality assurance manager stated that CSA officials were unaware these were sensitive positions because the contract did not define them as positions that required a security clearance; however, CSA officials admitted that they did not comply with the SOW requirements. The QAR noted that several contractor employees were removed from their positions or moved into other positions until they acquired security clearances. The DCMA audit reports showed that CSA officials implemented corrective actions on this issue; however, 20 contractor employees still did not have clearances for their positions as of October 12, 2009. According to the DCMA audit, these contractor employees worked in the ammunition supply point, a restricted area. Further, the QAR informed us that DCMA officials expected this to be resolved by the end of the year, and, as the contractor had operated without the clearances for the past 10 years, that a few more weeks would not hurt. The QAR stated that there would be a huge impact to the mission if the contractor employees were removed from their positions.

While DCMA officials identified issues with security clearances that had gone undetected for several years, per DCMA's Theater Quality Plan, DCMA officials should have issued a CAR in response to these findings. However, the DCMA QAR informed us that a CAR was not issued for the security findings because the issue was identified in a CSA corrective action plan. The QAR stated that the contractor's corrective actions were developed in response to its own internal reviews, but somehow got tied to a DCMA level III CAR. DCMA officials closed the level III CAR in September 2009, stating CSA officials completed all of the actions identified in its corrective action plan. However, DCMA's audit reports clearly showed that contractors without the required security clearance were still an issue 1 month later in October 2009. Further, CSA officials still had employees working without the required security clearance.

DCMA officials did not conduct oversight of this issue in accordance with its Theater Quality Plan. Based on DCMA's audit reports, DCMA repeatedly pointed out issues with contractor employees not having the required security clearance; however, DCMA officials did not hold CSA officials responsible or impose any penalties for not fully addressing the issue. Although DCMA identified security issues, DCMA failed to issue a

CAR to address these issues or to notify the contractor. Further, DCMA officials reported that they verified the completion of CSA's corrective actions related to the security issue before the issue was resolved. Lastly, no one verified that these employees were no longer working with sensitive information. The fact that there were still contractors in sensitive positions without security clearances is not acceptable and poses a security risk for military, civilian, and contractors in Kuwait. DCMA should assign a subject matter expert who is proficient in installation security as the QAR because security is a large part of the CSSC-K contract requirements.

Contractors Accessing Bases Without Common Access Cards

In addition to having a security clearance, CSA contractor employees must also have a CAC. DOD 5200.08-R "Physical Security Program," April 9, 2007, incorporating change 1, May 27, 2009 states that the CAC must be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces. RICC officials stated that under the Defense Cooperation Agreement with the Army of the State of Kuwait, installation access cards are used to access the military bases. However, we reviewed the agreement and did not find an alternative identification requirement. Therefore, the RICC officials should ensure that employees access the bases as required by DOD regulations. We requested that the Defense Manpower Data Center query the Defense Enrollment Eligibility and Reporting System[3] for the 36 contractor employees who were identified as not having a clearance. Specifically, we requested CAC information for the 21 contractor employees without a security clearance, the 11 employees whose clearance was in a hold or interim declined status, and the 4 employees with missing security files. We could not review CACs for the 20 employees known by the contractor and DCMA to occupy sensitive positions without security clearances because neither DCMA nor CSA officials provided us with the names for these employees, and they were not reflected on CSA's list of employees in sensitive positions or the SCAR. Based on the query of the 36 employees, 28 had a CAC, 5 did not have a CAC, and 3 had an expired CAC.

Even though all employees with access to military bases are required to have a CAC, the 28 employees who had a CAC occupied sensitive positions without a security clearance. These 28 employees occupied positions such as Theater Redistribution Center inspectors, supply technicians, and systems administrators. If the employee CAC does not have the proper restrictions, these employees could potentially gain access to restricted areas on the military base or to information systems with sensitive information using their CACs without the required security clearance. DCMA has noted in its audit reports that contractor employees without the required security clearance have had access to restricted areas, such as the ammunition supply point or theater storage area. These improper accesses would compromise the physical and logical access controls of the

[3]The Defense Enrollment Eligibility and Reporting System is a central repository for information collected on DOD personnel, including whether an individual has a CAC.

military base and information. Therefore, CSA officials should remove these employees from their positions if they do not have a security clearance.

Four of the five employees with no CACs were working as force protection officers with the remaining employee working as a supply technician. Of the five employees who did not have a CAC, three employees had a clearance in a hold status, and two employees had no evidence of a clearance. Force protection officers monitor employees coming onto and leaving the military base and need base access to do their job. Not only did they not have the CAC required for base access, they did not have the security clearance required for their positions. While the SOW indicates that all force protection officers do not require a security clearance, it states they must possess the security clearance equal to the level of classification they safeguard. Therefore, some force protection officers must have a security clearance. While these individuals were included on CSA's human resource list as requiring a security clearance, they did not have the required clearances, which is a security violation. Force protection officers must have a valid security clearance and CAC since they are the first defense for the military base personnel security and safety.

The three employees with an expired CAC had no evidence of a security clearance. These three employees were working as supply technicians, which CSA officials identified as a sensitive position. As with the force protection officers, these employees require access to the military bases. Not only did these employees not have the required security clearance to work in their positions, they did not have a valid CAC required to gain access to the military base. The PCO should direct CSA officials to remove these employees from their positions.

We provided the 36 employee names (21 contractor employees without clearances, 11 contractor employees without valid clearances, and 4 contractor employees with missing security clearance files) to both DCMA and RICC officials and informed them that corrective action must be taken to remove these individuals from their sensitive positions. Employees without valid security clearances may have access to sensitive or classified information that could cause grave damage to national security if not protected. Additionally, the integrity of military base security is compromised if these employees gained access to the military base without a CAC. Further, since the contractor employees identified were working in positions without the required security clearances, the PCO should conduct a review of the labor rates paid to those employees to verify that CSA officials did not bill the Army based on work they were not qualified to do because of a lack of security clearance.

Conclusion

CSA officials did not obtain and maintain contractor security clearances in accordance with the contract and did not track all sensitive positions. As a result, security violations occurred, CSA officials were in violation of the contract, and appropriate remedies should be considered. Further, DCMA did not conduct adequate oversight of CSA's security program, and the Army did not ensure that all contractor employees had a CAC required for access to the military bases. Therefore, CSSC-K contractor employees

occupied sensitive positions in Kuwait without appropriate security clearances and CACs, which was a security violation. If the Army does not ensure that all contractor employees have the required security clearances and maintain proper security information, these employees pose a threat to the military, civilian, and U.S. contractor personnel in Kuwait, as well as to national security. These issues are timely and relevant in identifying security concerns that the PCO must ensure are correctly implemented in the new Kuwait Base Operation Security Support Services, Ammunition Supply Point, and Supply Support Activity contracts.

Management Comments on the Finding and Our Response

See Appendix B for a summary of unsolicited management comments from the Provost Marshal Office, Area Support Group-Kuwait, on the finding and our response.

Recommendations, Management Comments, and Our Response

The Executive Director, U.S. Army Contracting Command, endorsed the comments provided by the Acting Executive Director, Rock Island Contracting Center.

1. We recommend that the Rock Island Contracting Center procuring contracting officer:

a. Conduct a 100-percent review of all positions related to work on the Combat Support Services Contract-Kuwait contract and document whether a security clearance is required in accordance with DOD 5200.2-R, "Personnel Security Program," updated February 23, 1996, and Army Regulation 380-67, "Personnel Security Program," September 9, 1988.

Rock Island Contracting Center

The Acting Executive Director, Rock Island Contracting Center, agreed. The Acting Executive Director stated that he will request Defense Contract Management Agency officials to initiate a 100-percent review of all positions with an estimated completion date of September 10, 2010. The Defense Contract Management Agency personnel will coordinate their review with the Army Support Group Provost Marshal's office and other security matter experts.

Our Response

The Acting Executive Director, Rock Island Contracting Center, comments are responsive, and no further comments are required.

b. Require that Combat Support Associates, with oversight from the Defense Contract Management Agency-Kuwait, conduct a review to validate that all contractor employees working in sensitive positions on the Combat Support Services

Contract-Kuwait contract have a valid security clearance, and if not, immediately remove that individual from his or her position.

Rock Island Contracting Center

The Acting Executive Director, Rock Island Contracting Center, agreed. The Acting Executive Director stated that he will request Defense Contract Management Agency officials to validate that all contractor employees working in sensitive positions have valid security clearances and will direct the contractor to remove any employee without a clearance from their position. The Acting Executive Director provided an estimated completion date of September 30, 2010.

Our Response

The Acting Executive Director, Rock Island Contracting Center, comments are responsive, and no further comments are required.

c. Conduct a review of the money paid to Combat Support Associates on the Combat Support Services Contract-Kuwait contract for employees that did not have security clearances and take the proper contractual remedies to recoup any money paid for employees who should have possessed a clearance but did not.

Rock Island Contracting Center

The Acting Executive Director, Rock Island Contracting Center, agreed and stated that Rock Island Contracting Center officials would consider if recoupment is appropriate based on the reviews requested in Recommendations 1.a and 1.b.

Our Response

The Rock Island Contracting Center, Acting Executive Director, comments are responsive, and no further comments are required.

d. Require Combat Support Associates to conduct reviews to validate that all of the sensitive positions on the Combat Support Services Contract-Kuwait contract are included in both the human resources lists and the security clearance access roster.

Rock Island Contracting Center

The Acting Executive Director, Rock Island Contracting Center, agreed. He stated that Rock Island Contracting Center officials, with Defense Contract Management Agency officials, will direct the contractor to conduct a review and validate sensitive positions to be captured on both the human resources lists and security clearance roster. The estimated completion date is September 30, 2010.

Our Response

The Acting Executive Director, Rock Island Contracting Center, comments are responsive, and no further comments are required.

e. Prohibit Combat Support Associates from creating "mirror" positions.

Rock Island Contracting Center

The Acting Executive Director, Rock Island Contracting Center, agreed. However, the Acting Executive Director stated that Rock Island Contracting Center officials have no evidence to prove that the contractor is creating mirror positions. The Acting Director stated that the Rick Island Contracting Center officials, along with the Defense Contract Management Agency officials, will direct the contractor to refrain from any practice of creating mirror positions.

Our Response

The Acting Executive Director, Rock Island Contracting Center, comments are responsive, and no further comments are required.

f. Pursue debarment against the contractor in accordance with Federal Acquisition Regulation Subpart 9.406, "Limitations," for not complying with the terms of the Combat Support Services Contract-Kuwait contract.

Rock Island Contracting Center

The Acting Executive Director, Rock Island Contracting Center, agreed and stated that issues identified during the requested reviews will be addressed and, if improper practices are identified, then Rock Island Contracting Command officials will take appropriate action.

Our Response

The Acting Executive Director, Rock Island Contracting Center, comments are responsive, and no further comments are required.

g. Coordinate with the Provost Marshall's office to conduct a review to determine whether all Combat Support Associate employees have a common access card as required by DOD 5200.08-R, "Physical Security Program," April 9, 2007, incorporating change 1, May 27, 2009. Remove Combat Support Associate employees without a current common access card from their position until they obtain a current common access card. Further, require employees who were removed from their positions because they did not have a clearance to turn in their common access cards.

Rock Island Contracting Center

The Acting Executive Director, Rock Island Contracting Center, agreed and stated that Rock Island Contracting Center officials will coordinate with the Army Support Group-Kuwait Provost Marshal's Office to conduct a review of contractor employee common access cards. The Acting Executive Director provided an estimated completion date of September 30, 2010.

Our Response

The Rock Island Contracting Center, Acting Executive Director, comments are responsive, and no further comments are required.

2. We recommend that the Commander, Defense Contract Management Agency-Kuwait:

a. Require quality assurance representatives to conduct quarterly reviews of contractor security files or the Joint Personnel Adjudication System to validate that all contractor employees in sensitive positions have the required security clearance and supporting documents as required in the Combat Support Services Contract-Kuwait contract and DOD 5200.2-R and document the reviews.

Defense Contract Management Agency-Kuwait

The Commander, Defense Contract Management Agency-Kuwait, agreed. The Commander stated that although the Defense Contract Management Agency does not have the personnel to perform quarterly security file reviews, he stated that Defense Contract Management Agency-Kuwait officials would coordinate and document quarterly reviews of the Joint Personnel Adjudication System.

Our Response

The Commander, Defense Contract Management Agency-Kuwait, comments are responsive. The quarterly reviews of the Joint Personnel Adjudication System in conjunction with the 100-percent review of all positions identified in Recommendation 1.a should validate and correct errors found in security requirements. No further comments are required.

b. Validate that quality assurance representatives issue and appropriately resolve corrective action requests in accordance with the Defense Contract Management Agency's Theater Quality Plan.

Defense Contract Management Agency-Kuwait

The Commander, Defense Contract Management Agency-Kuwait, agreed. The Commander stated that the Defense Contract Management Agency will issue corrective actions in accordance with its Theater Quality Plan, when required. However, the Commander stated that the Defense Contract Management Agency-Kuwait will allow the contractor to self-monitor low-risk areas and internally identified corrective actions so as not to deter the contractor from self-reporting. The Commander agreed that a corrective action request should have been issued for the security clearances due to the risk of non-compliance.

Our Response

The Commander, Defense Contract Management Agency-Kuwait, comments are responsive, and no further comments are required.

c. Assign a subject matter expert proficient in installation security as the Quality Assurance Representative for the surveillance of the security program.

Defense Contract Management Agency-Kuwait

The Commander, Defense Contract Management Agency-Kuwait, agreed. The Commander stated that the Defense Contract Management Agency-Kuwait did not have personnel with specific installation security experience so he will request that a subject matter expert be assigned to help the Defense Contract Management Agency. However, the Commander stated that there was no guarantee that Defense Contract Management Agency-Kuwait will receive the requested subject matter expert.

Our Response

The Commander, Defense Contract Management Agency-Kuwait, comments are partially responsive. The Commander should provide a plan of action to mitigate the risk if the Defense Contract Management Agency-Kuwait does not get a person with installation security experience. The Commander should provide his plan by October 22, 2010.

Appendix A. Scope and Methodology

We conducted this performance audit from August 2009 through June 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This is one in a series of audit reports on the management and administration of the CSSC-K contract (DASA02-99-C-1234). To determine whether the contractor properly managed and administered the CSSC-K contract, we interviewed officials involved in the management and oversight of the contract, reviewed the contract and supporting files, and reviewed documents as described below. Specifically, we visited the following locations:

- Rock Island Contracting Center, Rock Island, Illinois;
- DCMA International, Alexandria, Virginia;
- DCMA-Houston, Houston, Texas;
- DCMA-Kuwait, Camp Arifjan, Kuwait; and
- CSA Kuwait offices, Camp Arifjan, Kuwait.

We focused this report on CSA's security program and the management and oversight of contractor employees with security clearances. We reviewed Federal Acquisition Regulations, DOD Directive 5200.2, DOD 5200.2-R, AR 380-67, and the SOW to determine the requirements for security programs and for obtaining contractor security clearances. We also reviewed the contract and contract modifications, to include the SOW, as of December 2009, to determine whether the PCO identified which positions were sensitive positions and required security clearances.

We reviewed CSA's human resources list of all 379 contractor employees with security clearances, as of November 2009, in sensitive positions and CSA's November 2009 SCAR to determine whether all contractor employees in sensitive positions had the required security clearance. We also requested that the Defense Manpower Data Center query the Defense Enrollment Eligibility and Reporting System for the contractor employees without a security clearance, the employees whose clearance was in a hold or interim declined status, and employees without a security file to determine whether all contractors had a CAC as required in DOD 5200.08-R.

We used a judgmental sample to select names from CSA's SCAR and reviewed the supporting security file for those individuals to determine whether CSA officials maintained the documents required in DOD 5200.2-R and CSA's standard operating procedures for all employees with a security clearance. We judgmentally selected every tenth employee starting with the fourth employee name from the SCAR containing 379 employees. We also selected employees from the SCAR who had a clearance in a hold or interim declined status. Our sample resulted in 49 contractor employees. We

reviewed each file for the documents required in DOD 5200.2-R and CSA's standard operating procedures. We also interviewed a DCMA QAR to determine whether DCMA conducted oversight of contractors with security clearances.

We reviewed DCMA's monthly audit reports from May 2009 to October 2009 for QAR audits for those that related specifically to employees without security clearances. We followed up with the QAR on specific reports and obtained the related CAR, CSA's corrective action plan, and CSA's internal CAR. Then we reviewed the documents to determine whether CSA and DCMA officials took the appropriate actions to correct the issue of employees in sensitive positions without security clearances.

Lastly, we obtained the names of contractor employees who require security clearances during a tour of CSSC-K contract operations in Kuwait. We reviewed CSA's human resources list of employees in sensitive positions to determine whether all employees were on the list. We also interviewed DCMA QARs to determine whether DCMA reported any security issues identified as required in its Theater Quality Plan.

Use of Computer-Processed Data

We relied on computer-processed data from the Defense Enrollment Eligibility Reporting System to determine whether a sample of contractor employees had a CAC. We did not assess the reliability of the database because it would not affect materiality of our findings or recommendations. Our objective was to determine whether the contractors had a security clearance, not to determine the reliability of the Defense Enrollment Eligibility Reporting System outputs used in the process. We did not perform any detailed reliability testing of the Defense Enrollment Eligibility Reporting System data. Regardless of whether the contractors had a CAC, we would still make the same recommendations to remove all contractors without a security clearance.

Prior Coverage

During the last 5 years, the Army Audit Agency issued one report discussing the CSSC-K contract. Unrestricted Army reports can be accessed from .mil domains over the Internet at https://www.aaa.army.mil/.

Army

Army Audit Report No. A-2009-0132-ALL, "Contracting Operations: U.S. Army Contracting Command Southwest Asia – Kuwait," September 26, 2009

Appendix B. Management Comments and Our Response

Provost Marshal Office Comments

Although not required to comment, the Provost Marshal, Area Support Group-Kuwait, provided comments that were included with those from DCMA-Kuwait. The Provost Marshal commented that force protection officers are not required to have a security clearance or CAC. The Provost Marshal stated that, in accordance with AR 380-67, "Personnel Security Program," September 9, 1988, contractors assigned to military police or provost marshal duties are noncritical sensitive positions. He stated that this applied to law enforcement officials and not force protection officers. The Provost Marshal also stated that force protection officers are required only to have a favorable National Agency Check, not a security clearance in accordance with AR 380-67.

The Provost Marshal further stated that Area Support Group-Kuwait installations are not federally controlled facilities, but are provided by the Kuwaiti Government under the Defense Cooperation Agreement. The Provost Marshal stated that, in accordance with the agreement, the installations comply with the use of installation access cards, which is composed of biometric screening, passports, visas, and other requirements to work in Kuwait. He further stated that the majority of the contracted workforce in Kuwait are third-country nationals who cannot get a CAC.

In addition, the Provost Marshal stated that the DOD IG report statements conflicts with AR 380-67 requirements because not all force protection officers are required to have a clearance. He further stated that a security clearance is not required for a contractor to obtain a CAC nor does the CAC ensure that proper security requirements are established in accordance with the guidelines.

Our Response

As stated on page 12, the SOW for the CSSC-K contract requires force protection officers to have a security clearance equal to the level of classification they safeguard. The SOW for the CSSC-K contract also requires the contractor to maintain a list of the personnel who require a security clearance, and the contractor is bound to those contract terms. The force protection officers referred to in this report were on the contractor's list of personnel required to have a security clearance, but they did not have the clearances.

As stated on page 11, we reviewed the Defense Cooperation Agreement provided to us, as did the DOD IG Legal Counsel, and we did not find a requirement for installation access cards. The agreement only required compliance with DOD guidelines. DOD 5200.08-R, "Physical Security Program," states that the CAC must be the principal identity credential for supporting interoperable access to installations, facilities, buildings, and controlled spaces. It does not specify federally controlled installations. Further, our report did not state that a security clearance is required to have a CAC; we

stated that personnel with a CAC who do not have a security clearance could gain access to sensitive information by using their CAC if the proper controls were not implemented.

Rock Island Contracting Center Comments

DEPARTMENT OF THE ARMY
U.S. ARMY CONTRACTING COMMAND
9301 CHAPEK ROAD
FORT BELVOIR, VA 22060-5527

REPLY TO
ATTENTION OF:

AMSCC-IR

AUG 13 2010

MEMORANDUM FOR [redacted] Internal Review and Audit Compliance Office, Headquarters, U.S. Army Materiel Command, [redacted]

SUBJECT: Kuwait Contractors Working in Sensitive Positions Without Security Clearances or Common Access Cards (CACs) (Project No. D2009-D000AS-02666.000) (D0950)

1. References:

a. Memorandum, Rock Island Contracting Center, CCRC, 30 June 2010, subject: same as above (enclosed).

b. Memorandum, DODIG, 25 June 2010, subject: same as above.

c. Draft Report (D2009-D000AS-02666.000), DODIG, undated, subject: same as above.

2. Having reviewed the documents at references 1b and 1c, the U.S. Army Contracting Command concurs with the comments within reference 1a.

3. The ACC point of contact is [redacted]

Encl

JEFFREY P. PARSONS
Executive Director

Printed or Recycled Paper

UNCLASSIFIED

DEPARTMENT OF THE ARMY
ROCK ISLAND CONTRACTING CENTER
1 ROCK ISLAND ARSENAL
ROCK ISLAND, IL 61299-8000

REPLY TO
ATTENTION OF:

CCRC

MEMORANDUM FOR Inspector General Department of Defensece, 400 Army Navy Drive, Arlington, VA, 22202-4704

SUBJECT: Kuwait Contractors working in Sensitive Positions without Security Clearances or CACs (Project No D2009-D000AS-02666.000)

1. Thank you for the opportunity to review the draft report. Our comments are enclosed.

2. The POC is [redacted]

Michael R Hutchison 30 JUL 10

ENCL

MICHAEL HUTCHISON
Acting Executive Director
Rock Island Contacting Center

UNCLASSIFIED

Encl

DoDIG Draft Report: Kuwait Contractors Working in Sensitive Positions without Security Clearances or CACs

Recommendations for RICC.

1. *We recommend that the Procuring Contracting Officer:*

a. Conduct a 100 percent review of all positions related to work on the Combat Services Contract-Kuwait contract and document whether a security clearance is required in accordance with DOD Regulation 5200.2-R, "Personnel Security Program," updated February 23, 1996, and Army Regulation 380-67, "Personnel Security Program," September 9, 1988.

RICC comments. Concur. RICC will request DCMA to initiate a 100 percent review of all positions and document whether a security clearance is required in accordance with applicable DOD and Army regulations. DCMA will coordinate its review with Army Support Group (ASG) Kuwait Provost Marshall's office and other security subject matter experts. Estimated completion date of the review is September 10, 2010.

b. Require that Combat Support Associates, with oversight from the Defense Contract Management Agency-Kuwait, conduct a review to validate that all contractor employees working in sensitive position on the Combat Support Services Contract-Kuwait contract have a valid security clearance, and if not, immediately remove that individuals from his or her position.

RICC comments. Concur. RICC will request DCMA validate that all CSA employees working in sensitive positions have valid security clearances. If applicable, RICC and DCMA will direct CSA to immediately remove employees that do not have the appropriate clearance for their position. Estimated completion date is September 30, 2010.

c. Conduct a review of the money paid to Combat Support Associates on the Combat Support Services Contract-Kuwait contract for employees that did not have without a security clearance and take the proper contractual remedies to recoup any money paid for employees who should have possessed a clearance but did not.

RICC comments. Concur. Based on reviews conducted in paragraphs 1.a. and b. above, RICC will determine if recoupment is appropriate.

d. Require Combat Support Associates to conduct reviews to validate that all the sensitive positions on the Combat Support Services Contract-Kuwait contract are included in both the human resources lists and the security clearance access roster.

DoDIG Draft Report: Kuwait Contractors Working in Sensitive Positions without Security Clearances or CACs

RICC comments. Concur. RICC and DCMA will direct CSA to conduct a review and validate sensitive positions to be captured on both the human resources lists and security clearance roster. Estimated completion date is September 30, 2010.

e. Prohibit Combat Support Associates from creating "mirror" positions.

RICC comments. Concur. At this time, RICC has no evidence to indicate that CSA is creating "mirror" positions. RICC and DCMA will, however, direct CSA to refrain from any practice of creating "mirror" positions.

f. Pursue debarment against the contractor in accordance with Federal Acquisition Regulation Subpart 9.406, "Limitations," for not complying with terms of the Combat Support Services Contract-Kuwait contract.

RICC comments. Concur. Information pertaining to the reviews, above will be assessed, and if improper practices are identified, RICC will take appropriate actions as necessary.

g. Coordinate with the Provost Marshall's office to conduct a review to determine whether all Combat Support Associate employees have a common access card as required by DOD 5200.08-R, "Physical Security Program," April 9, 2007, incorporating change 1, May 27, 2009. Remove Combat Support Associate employees without a current common access card from their position until they obtain a current common access card. Further, require employees who were removed from their positions because they did not have a clearance to turn in their common access card.

RICC comments. Concur. RICC will coordinate with Army Support Group-Kuwait (ASG-KU) Provost Marshall Office to conduct a review. Estimated completion date September 30, 2010.

Defense Contract Management Agency Comments

DEFENSE CONTRACT MANAGEMENT AGENCY
DCMA MIDDLE EAST - KUWAIT
APO AE 09366

IN REPLY
REFER TO: Commander, DCMA-Kuwait

26 Jul 2010

MEMORANDUM FOR Department of Defense Office of Inspector General

SUBJECT: DCMA-Kuwait Response to DODIG DRAFT Audit "Kuwait Contractors Working in Sensitive Positions Without Security Clearances or CACs (Proj. No. D2009-D000AS-0266.000)"

1. Attached is DCMA-Kuwait Commander's response to the subject draft audit. Contained herein are responses to Recommendations 2.a-c.

2. Also attached are comments to the audit provided by Calvin Foster, Commander, USN, the Provost Marshal for Area Support Group-Kuwait.

3. Please address all questions to Michael Whalen, Lt Col, USAF, at [redacted]

Michael R. Whalen, Lt Col, USAF
Commander

Attachments :
1. DCMA Commander Response
2. Provost Marshal Response
3. AR 190-56
4. AR 380-67

2. Commander, DCMA

a. Require quality assurance representatives to conduct quarterly reviews of contractor security files or the Joint Personnel Adjudication System to validate that all contractor employees in sensitive positions have the required security clearance and supporting documents as required in the Combat Support Services Contract-Kuwait contract and DOD 5200.2-R and document the reviews.

Concur:

While DCMA is not manned to conduct quarterly reviews of all contractor security files according to the contractor's Standard Operating Procedures, DCMA can coordinate quarterly reviews in JPAS to validate sensitive positions have the required security clearances. DCMA will document the reviews.

b. Validate QAR issues and resolve CARs in accordance with DCMA's Theater Quality Plan.

Concur:

DCMA will issue CARs per the TQP when the accompanied risk rating so requires. DCMA has opted to allow the contractor to self-police some of its self-identified Internal CAR (ICAR) when associated risk is low. If DCMA were to write a CAR for every ICAR the contractor has self-identified, this could deter the contractor from self-reporting problems. In the case of security clearances, however, DCMA concurs that a DCMA CAR should have been issued as opposed to simply monitoring the contractor's ICAR due to the risk associated with no-compliance.

c. Assign a subject matter expert proficient in installation security as the Quality Assurance Representative for the surveillance of the security program.

Concur with Comments:

DCMA Kuwait will request a Subject Matter Expert (SME) with background in Installation Security be assigned. However, since DCMA does not have in-house personnel with this type of experience, we will have to request assistance from the Services. There is no guarantee that a SME will be provided by the Services.

Provost Marshal Office, Area Support Group-Kuwait

The following has been submitted to DCMA by [redacted] Commander, USN, the Provost Marshal for Area Support Group Kuwait:

Reference page 3 - force protection officers being required to have a security clearance and use of Common Access cards.

Per DODI 5210.90 dtd 9 Jul 07, The Secretary of Defense assigned the Secretary of the Army as the executive agent for training, certification and physical fitness standards for security guards. The Army's regulation for employment and qualifications is covered under AR 190-56 "The Army Civilian Police and Security Guard Program."

CSSC-K contractors assigned to military police/Provost Marshal type duties are deemed to fill a noncritical-sensitive position as outlined in AR 380-67 3-101(2). This applies to law enforcement type positions, and not to force protection officers. All personnel assigned to law enforcement and dispatch duties do have a valid clearance. In addition, as a precaution, the Provost Marshal runs random JPAS checks on personnel in these positions as part of their audits. In the past 2 years, they have not found one person assigned to dispatch, law enforcement, or FPO duties guarding areas that require a clearance to be in violation of the AR 380-67.

Force Protection Officers fall under section AR 380-67 3-612 which requires US personnel to have a favorable NAC, not a security clearance as in the report. This is also stated in AR 190-56 2-3. AR 380-67 3-201.1 lists and exception for non-US personnel in which allows for the use of the local country's version local law enforcement and national check.

ASG-KU installations are not Federally controlled facilities. All installations in Kuwait are provided for or allowed by the Kuwaiti government under the Defense Cooperation Agreement. The installations comply with the Area Support Group Installation Access Policy, along with the laws and agreements with the State of Kuwait both verbal and in writing, are the basis of the establishment of the installation access card utilize. The installation access card utilizes biometric screening, passports, visa's and other required documents to work in the State of Kuwait. The utilization of CAC cards does not allow the USG to comply with Kuwaiti work requirements. In addition, the majority of the contracted work force in the State of Kuwait is Third Country Nationals, to include the work force provided by the Kuwaiti government, that cannot get CAC cards.

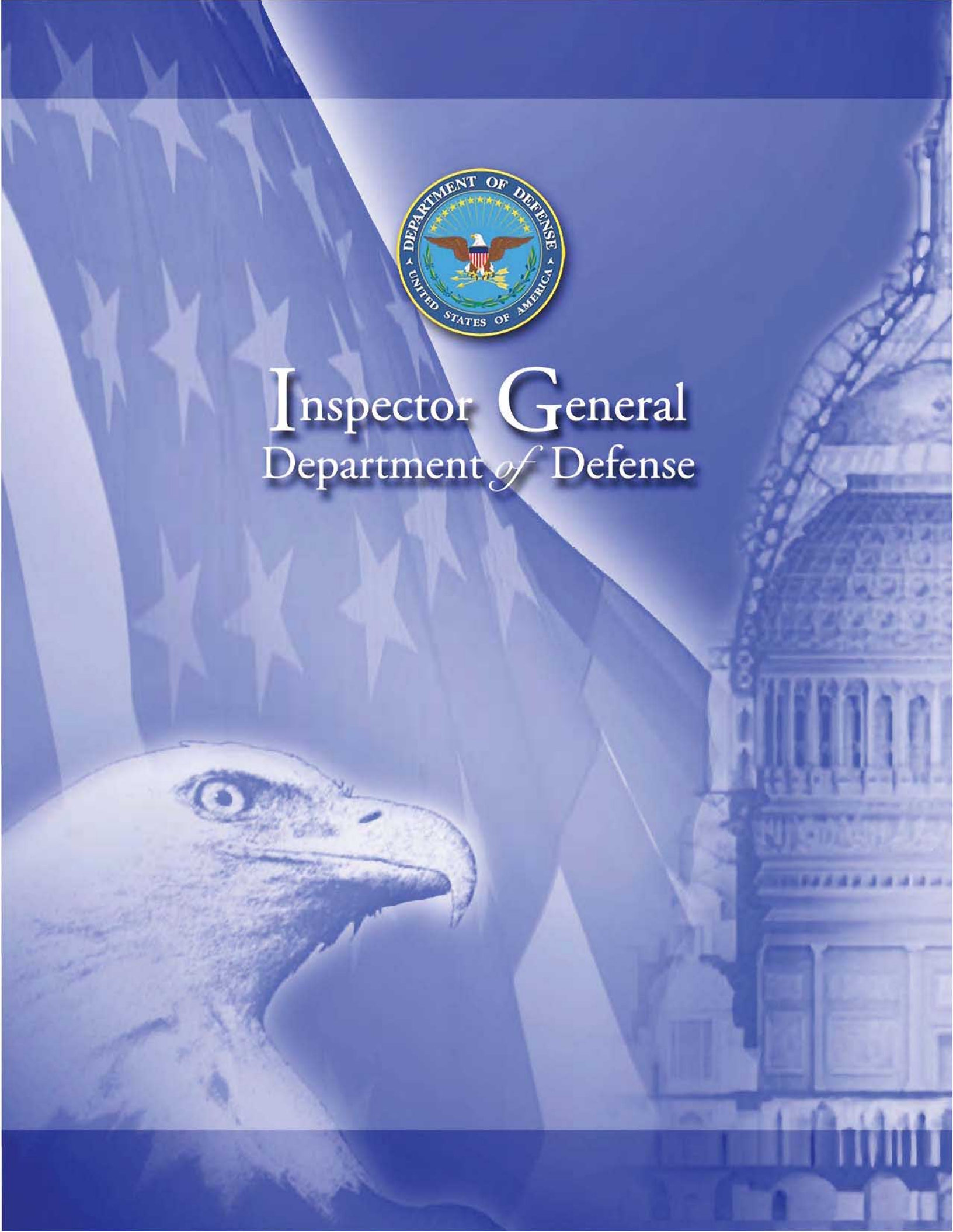
The Deputy Secretary of Defense Directive Type Memorandum 08-006 "DoD Implementation of Homeland Security Presidential Directive 12 (HSPD-12), requires the migration to a single identification standard for Federal Employees under the terms of applicable contracts, for physical access to all Federally controlled facilities and logical access to Federally controlled information systems.

DTM-08-006 pg 2 states that the CAC can be used for logical and physical access once access privileges are granted. It does not state that it has to be nor does it limit a commander's ability to utilize other systems as deemed necessary to meet mission requirements. The installation access card is utilized by ASG to ensure that all personnel authorized access to the installations meet Kuwaiti

requirements to be/work in the State of Kuwait. The CAC is utilized to control those who have access to the NIPR computer systems and is conducted within DMDC guidelines.

Reference page 12, the DOD IG contradicts itself on what it is saying to what the instructions state. Not all force protection officers are required to have clearances, only those guarding facilities/areas outlined in AR 380-67. Background and credit checks are conducted during the contractor's hiring procedures.

In addition, a security clearance is not required to have a CAC card issued nor does having a CAC card ensure proper local security requirements that are established IAW applicable guidelines, legal reviews and Army approved procedures.



Inspector General
Department of Defense